

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

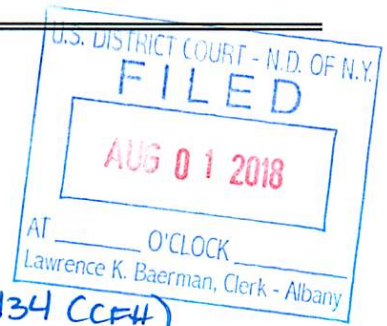
United States of America)

v.)

Xiaoqing Zheng, d/o/b xx/xx/1963)

Case No. 1:18-MJ-434 (CFH)

Defendant(s)



CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 5, 2018 in the county of Schenectady in the
Northern District of New York, the defendant(s) violated:

*Code Section**Offense Description*

Count 1: 18 U.S.C. § 1832(a)(1)

Theft of Trade Secrets

This criminal complaint is based on these facts:

☒ Continued on the attached sheet.

A handwritten signature in blue ink, appearing to read "M. McDonald".

Complainant's signature

FBI S/A M.D. McDonald

Printed name and title

Sworn to before me and signed in my presence.

Date: August 1, 2018

A handwritten signature in blue ink, appearing to read "Christian F. Hummel".

Judge's signature

City and state: Albany, New York

Hon. Christian F. Hummel, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

STATE OF NEW YORK)

) cc

COUNTY OF ALBANY)

I, M.D. McDonald, being duly sworn, depose and state that:

INTRODUCTION

Agent Background

1. I have been employed as a Special Agent of the FBI since 2002 and currently I am assigned to the Albany, NY field office where I work on the Counterintelligence Squad. During my 16 years of employment with the FBI, I have received training on investigative techniques and evidence recovery procedures, I have conducted many criminal investigations, and I have conducted many searches and arrests. I was employed for approximately 8 years (from 2011 through 2018) as a Supervisory Special Agent and Associate Division Counsel, where I oversaw the legal, ethics, and asset forfeiture programs for the Albany field office.
2. I am a licensed attorney and member of the Bar of the State of New York, having graduated from Albany Law School of Union University and admitted to the New York State Bar in 1998. During my 20 years as a lawyer, I have completed many continuing legal education courses of instruction, including courses focusing on ethics and criminal practice, and maintained my good standing as a licensed attorney.
3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). As a FBI Special Agent, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to the theft of trade secrets.
4. In accordance with my present duties, I make this affidavit in support of a criminal complaint charging Xiaoqing Zheng with a violation of 18 U.S.C. § 1832(a)(1) [Theft of Trade Secrets].
5. I make this affidavit from personal knowledge based on my participation in this investigation, and review of reports by myself and/or other law enforcement agents, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. The information outlined below is provided for the limited purpose of establishing probable cause and does not contain all details or all facts of which I am aware relating to this investigation.

SUMMARY OF THE INVESTIGATION

6. The trade secret(s) at issue in this case belong to General Electric's Power division and involves mathematical computations relating to sealing and optimization of turbines, in the form of MatLab (a high level computer language used for mathematical computing) and Excel (spreadsheet) files. GE considers this technology to be proprietary and has taken steps to keep its technology secret.

7. Xiaoqing Zheng, a Principal Engineer employed by GE at its GE Power facility in Schenectady, NY, is suspected of taking /stealing, on multiple occasions via sophisticated means, data files from GE's laboratories that contain GE's trade secret information involving turbine technology. In particular, Zheng is believed to have utilized elaborate means to conceal his removal of GE data files including conducting his activities after normal work hours, "staging" encrypted files in folders on his work (desktop) computer, using encryption to prevent GE from seeing the contents of the data files, using steganography to (in essence) hide data files in the binary code of another file (specifically a digital photograph), and e-mailing GE's data files to Zheng's personal e-mail address -----@hotmail.com.¹

8. Although the overall investigation relates to a broader scope of activities involving the suspected theft and unlawful use of GE's trade secrets, including Zheng's ownership interest in companies that may compete with GE and Zheng's contacts in China, the primary focus of this affidavit is Zheng's actions in 2018 in which he encrypted GE data files containing trade secret information, and thereafter sent the trade secret information from his GE work (desktop) computer to Zheng's personal e-mail address (-----@hotmail.com) hidden in the binary code of a digital photograph via a process known as steganography. Additionally, the secondary focus of this affidavit is Zheng's actions in 2014 in which he downloaded more than 19,000 files from GE's computer network onto an external storage device, believed by GE investigators to have been a personal thumb drive.

DETAILS OF THE INVESTIGATION

Background on Xiaoqing Zheng

9. Xiaoqing Zheng is a 56 year old U.S. citizen of Chinese descent. Zheng is also believed to have Chinese citizenship and to possess significant personal and professional contacts in China. Zheng has lived with his wife at their marital residence in Niskayuna, New York for several years. Zheng has degrees from Northwestern Polytechnical University and Massachusetts Institute of Technology in "aero engine" fields.

10. Zheng was hired by General Electric in 2008 to work as a Principal Engineer. Since being hired, Zheng has worked, full time, for GE's Power division in Schenectady County, NY. Zheng works on "Steam Turbine Flow Path" technology. This technology is used in many of the turbines that GE sells both domestically and internationally. In order to perform his duties, Zheng has been given a GE-issued laptop computer, a GE-issued desktop computer, a GE-issued smartphone (an iPhone), and a GE e-mail address. GE employees like Zheng are permitted to,

¹ Zheng's actual Hotmail e-mail address is available to the Court upon request.

and routinely do, take their GE-issued electronics home in order to work. Additionally, Zheng has disclosed to GE that he maintains a personal e-mail address of -----@hotmail.com.

11. According to GE, Zheng is the owner of a business entity (opened in 2015) called Nanjing Tainyi Aeronautical Technology, Ltd, located in Nanjing, China. Zheng disclosed this information to GE, and also disclosed to GE that he and “his brothers” own the company. Zheng has described the business as a “parts supplier for civil aviation engines.”

12. GE has conducted a conflict of interest analysis over Zheng’s Chinese company and determined that Zheng’s company posed at least three potential conflicts: (i) the company could sell parts to GE Aviation (a subsidiary of GE); (ii) the company could sell parts in competition to GE Aviation; and (iii) Zheng’s time spent working for his company could make him a less productive employee for GE. GE determined that Zheng’s “role is obviously more than just “owner” – he is responsible for development and implementation of new sealing technologies for his company.” However, GE did not instruct Zheng that his interest in the Chinese company was unacceptable, and Zheng was permitted to retain his GE employment.

Publicly Available Information on Zheng’s Chinese Companies

13. Although I am unable to determine much about Zheng’s company due to its location in China, a basic level Internet search shows that Zheng is (i) the “owner” and “chairman” of (a slightly differently named company) Tianyi Aviation Technology Co, Ltd., and (ii) the “general manager” of a separate company Lioning Tianyi Aviation Technology Co Ltd. According to publicly available Internet postings, Zheng’s Chinese companies “fill gaps” in technical fields in China in the aviation industry. According to some of the same postings, Zheng himself is described as a leader of a team of experts, and a person who has been involved in opening an industrial facility in China. Also according to the publicly available postings, Zheng was described as a 2012 selectee of the “Thousand Talents Program”. I know this program to be a Chinese government program designed to recruit highly educated researchers to bring their skills to China.

14. GE has noted that based on their review of the publicly available Internet sites relating to Zheng’s companies in China, it appeared he was working on the same types of technology for the Chinese companies that he is employed to work on by GE. The GE proprietary technologies on which Zheng works would have economic value to any of GE’s business competitors.

15. I reviewed publicly available publications on the Internet website tianyiseal.com, relating to Tianyi Aviation Technology, Co, and I observed a publication about the company’s efforts toward developing advanced turbine sealing technology. On the web page is a posting that reads, in pertinent part, “Sealing technology is the most effective way to improve engine efficiency... Low leakage advanced seals could cut in half the estimated 4% cycle air currently used to purge high pressure turbine cavities... It is a goal of NTAT to develop efficient manufacture technology to serve engine companies with low-cost, high-quality sealing products.” In essence, a company that Zheng appears to either own or manage is advertising in China its expertise in turbine sealing technology – the technology on which Zheng works on at

GE, and the technology that Zheng is believed to have egressed from GE's system while encrypted and hidden in a photograph.

GE Has Taken Steps to Protect its Turbine Sealing Trade Secrets

16. GE Power has taken substantial steps toward protecting its trade secret information relating to its turbine technologies. GE Power's facilities (at which Zheng works, and where Zheng encrypted the MatLab and Excel files, moved them to a "temp folder, renamed them, hid them within the binary code of his digital photograph, and e-mailed them to his personal Hotmail address) are access controlled utilizing perimeter security, as well as internal access control security. Visitors are required to register with security, wear visitor badges, and be escorted by approved personnel. Zheng has full access to the GE space in the GE Power facility. GE employees are required to sign proprietary information agreements, and they are advised of GE policies including the fact that any inventions or innovations they may create while a GE employee are the property of GE. Additionally all employees are subject to the GE Acceptable Use of GE Information Resources (AUGIR) which explains how to use and protect GE information.

17. To protect their sensitive data / trade secrets, GE employs multiple digital controls, including:

- a. Access Control – GE computing assets are protected by a centrally managed network/host login and authentication credentials. These credentials are granted to authorized employees and contingent workers based on their need to access company data.
- b. Banner warnings – GE computer systems contain banner style warning notices to advise GE employees that GE's computer system is available to them for work-related reasons and is subject to monitoring. GE advises employees that GE monitors employees' usage of its computer systems (which I and GE believe is the main reason Zheng encrypted the files he stored in temp folders on his computer, as GE would have been able to view the files Zheng was staging for egress had he left the files unencrypted).
- c. Ban on use of USB drives – In 2016 or 2017, GE instituted a policy restricting employees' use of external USB drives such as thumb drives, and GE took steps to ensure their computer system would not permit the use of thumb drives. This security measure prevents employees from downloading trade secret information to drives they could physically take with them (which is a reason why I and GE believe Zheng employed the complex measures he used to hide trade secret information in a digital photograph and utilize e-mail to egress it, as he could no longer utilize a thumb drive).

18. GE Power has general office policies on the use and handling of its confidential and proprietary information which are set out, for example, during training, in employee handbooks, through oral warnings at company meetings or conventions, and on signs or banners posted in

the workplace. GE has told me that it was clear to Zheng that he was not authorized to take the files he took, and that the files were undoubtedly GE's property. GE believes Zheng used such a complex process to encrypt, stage, hide and e-mail the MatLab and Excel files specifically because it was very clear that he was not permitted to take this data, and there was no plausible reason to go to such lengths to hide what he was doing if he believed the files were not trade secrets that he was not permitted to take or share with third parties.

GE's Identification of the Crimes Under Investigation

19. In 2014, GE corporate security learned that Zheng had copied 19,020 electronic files from one of his GE-issued computers onto a USB external storage device, believed to be a thumb drive. GE has been unable to determine the contents of the 19,020 files, however, it is suspected that the files related to Zheng's work for GE as employees are discouraged from using GE-issued electronics to conduct anything more than incidental personal business. GE investigators interviewed Zheng in 2014 regarding this incident, and Zheng told them that he had deleted the files. GE had no additional information about the downloaded files, nor any corroboration about whether the files had been deleted or shared with any third parties.

20. In November – December 2017, GE discovered that approximately 400 encrypted files had been saved on Zheng's work (desktop) computer. The files were encrypted using a program called Axcrypt – a program not used by GE. This practice was not standard for GE employees, and GE did not know why Zheng would be encrypting files on his work (desktop) computer. Due to the encryption, GE was unable to view the contents of the 400 files that Zheng encrypted and saved on his GE computer.

GE's Efforts to Monitor Zheng's Computer Activity

21. Following GE's discovery of the 400 encrypted files on Zheng's GE-issued computer, GE installed monitoring software on Zheng's computer(s) in an attempt to determine what information he was encrypting, and what he was doing with the information (e.g., transferring it elsewhere, etc.).

22. During the process of monitoring Zheng's activities on his computer(s), GE discovered that on or about July 5, 2018 Zheng moved approximately 40 encrypted files to a "temp folder" on his GE-issued work (desktop) computer. Since GE security personnel were monitoring Zheng's activities they were able to determine the password Zheng used for the encryption. GE determined that the files were MatLab and Excel files containing calculations relating to sealing and optimizing turbine technology – information that GE considers to be proprietary and secret.

23. In connection with GE's monitoring of Zheng's computer activities, GE learned that on July 5, 2018 Zheng used "steganography" (a means of hiding a data file within the code of another data file) to conceal data from the aforementioned 40 electronic files onto his GE-issued work (desktop) computer. Through the steganography technique, Zheng placed the aforementioned electronic files into the binary code of an innocuous looking separate electronic file on the computer - a digital photograph of a sunset. Zheng then e-mailed (using his GE e-mail address) the digital photograph file of the sunset (which secretly contained the hidden GE

electronic files containing GE's proprietary data) to his personal e-mail address of -----@hotmail.com. This action is detailed more thoroughly below in the portion of this Affidavit labeled "Steganography Egress Summary".

Steganography Egress Summary

24. On Thursday, July 5, 2018, at around 11:12 a.m., Zheng compressed 39 MatLab electronic files (MatLab is a computer programming language used for technical computing) and one Excel (spreadsheet) file into a new electronic file titled 'Optimizing.zip'. This activity occurred within file system path d:\users\204050598\documents\nti\2018\carbon\design tool\.

25. Then, using the software application Axcrypt (encryption software), Zheng encrypted the electronic file 'Optimizing.zip'. To do so he used a personal passphrase (NJI9*UHB).

26. Next, using Axcrypt, Zheng renamed the encrypted file "Optimizing.zip.axx" to 'F03B336A.axx'. According to GE, the word "optimizing" would appear to relate to turbine optimizing, which would seem to be work related files, but 'F03B336A' was not a file name that would have any connection to GE's proprietary trade secret information, so essentially Zheng used an innocent-looking name for the file.

27. Zheng then cut the encrypted file 'F03B336A.axx.' from d:\users\204050598\documents\nti\2018\carbon\design tool\ and pasted it into c:\tmp (described as a "temp" folder).

28. Around 5:17 p.m. on July 5, 2018, Zheng plugged an iPhone into his GE-issued work (desktop) computer. Zheng copied an image file 'IMG_2064.JPG' from the iPhone onto the desktop of his GE-issued work computer. Zheng then renamed this image as 'dawn.JPG'.

29. Zheng edited the 'dawn.JPG' (originally just a photograph of a sunrise or sunset with no text) image by typing "Happy Fourth of July" into the image. Zheng re-saved the image to the desktop of his GE-issued work computer. Zheng then cut the file from the desktop of his GE-issued work computer and pasted it into c:\tmp (the same folder in which Zheng had saved the 39 MatLab files and one Excel file).

30. Zheng then opened Cygwin Bash Shell (a text-style layer of computer programming language that understands and executes commands typed by users) and typed the commands "cd c:\tmp" and "dir" which listed the contents of the directory on the command line interface. Zheng then typed "vim -b dawn.jpg" which listed the binary code (essentially the "ones and zeros" used in computer programming) of the 'dawn.JPG' file. Zheng then typed in "88" at the end of the binary code. Next, Zheng typed "r: F03B336A.axx" which inserted a read-only copy of this encrypted file into the binary code of the 'dawn.JPG' file. Zheng then added "88" at the end of the new binary code. Essentially in this process, Zheng pasted the binary code for the 39 MatLab files and one Excel file (most, if not all, of which contained GE's proprietary information) at the end of the binary code for the digital photograph, with "88" (which I know to be widely viewed as a lucky number and symbol of good fortune in Chinese culture), thereby setting the GE-owned data apart from the innocent-looking digital photograph data.

31. Zheng returned to the Explorer Window within the c:\tmp and renamed the file 'F03B336A.axx' to 'de.dat', then shredded and deleted the file through the AxCrypt application. Changing the .axx (Axcrypt) file extension to .dat (data file) extension is significant, as GE explained that a .dat file would seem to be a routine file type that would not draw attention. Through this process, Zheng deleted the data from his "temp" folder, as the data had been hidden in the binary code of the digital photograph.

32. At 5:29 p.m. on July 5, 2018, Zheng attached the file "dawn.JPG" to a message in his GE Outlook e-mail account, typed "Nice view to keep" into the subject line of the e-mail, and sent the e-mail with the attachment from his GE e-mail address to -----@hotmail.com. In this process, Zheng sent the digital photograph (with the GE-owned files hidden in the binary code) to his personal e-mail address – completing the process of "egressing" or taking the GE-owned proprietary information from the GE computer system and sending it to his Hotmail account, stored on Microsoft Online Services' servers where he could retrieve it from an outside location.

33. In essence, Zheng took great care to conceal what he was doing with GE's proprietary data files, and he not only hid the data he was staging in a "temp folder" by encrypting it so GE could not see what files he was saving, but he also used steganography to hide the fact that he sent GE's data to his personal e-mail address (i.e. concealing the data within the binary code of the digital photograph). A person tasked by GE with routine e-mail monitoring would have seen the digital photograph in Zheng's GE e-mail, but unless he/she knew where to look within the binary code of the digital photograph, he/she would only have seen a photograph of a sunset. Zheng's use of encryption and steganography techniques are both uncommon and serve no apparent purpose but for concealing his activities from his employer.

34. Zheng's actions (moving the files, renaming them, encrypting them, and hiding them within the binary code of seemingly harmless files) are uncommon even among trained computer experts, and both GE Digital analysts and FBI agents specializing in cyber crimes have told me that they were aware of these measures in theory, but that they had never actually seen a subject employ them. GE provided investigators real-time video of Zheng's computer activities on July 5, 2018, and the entire process took Zheng less than 10 minutes. Based on my experience and training, including my discussions with FBI Agents who specialize in cyber crimes, the fact that Zheng accomplished this complex process so quickly and easily makes it highly probable that he had practiced these techniques and utilized them in the past.

35. According to GE, Zheng is in possession of at least the following mobile electronic items: an HP Elite Laptop computer and an iPhone X. And, according to GE, Zheng downloaded over 19,000 files from the GE computer system onto an external USB device, believed by GE to be a thumb drive.

Common Practices Involving Stolen Trade Secrets

36. Based on my training and experience, I am aware that once trade secret information / data is egressed from the lawful owner's computer system (e.g. on a thumb drive or via e-mail), the stolen trade secret information can easily be stored and saved on a wide variety of electronic storage devices such as laptop or desktop computers, cellular telephones, iPads or similar tablet

style devices, thumb drives, and other devices containing electronic storage capabilities. Once the stolen trade secret information has been egressed, the information can be used by, sold to, exchanged with, traded to, etc. individuals and entities who are looking to illegitimately acquire the information.

37. Based on my training and experience, I know that there is a market in China comprised of individuals and businesses who are willing to pay money for trade secret information / data stolen from U.S. companies. Some of these individuals and businesses are willing to pay more money than others, thus an individual who first possesses stolen trade secret information may 'shop' the stolen trade secret information in an effort to obtain the most money. Such an individual's 'shopping' of the stolen trade secret information takes time and requires the individual to maintain the stolen trade secret information in a format that preserves the stolen information.

Execution of a Search Warrant at Zheng's Niskayuna, New York Residence

38. On August 1, 2018, agents with the FBI executed a federal search warrant at Zheng's residence in Niskayuna, New York. Agents were authorized to search for, and seize, evidence involving the theft of trade secrets from GE.

39. In connection with the above-referenced search, agents seized:

- a.) a handbook that explains the type of resources the government of China will give to individuals or entities who can provide certain technologies;
- b.) Zheng's passport showing five international trips to China in the past two years; and
- c.) various electronic items of which forensic examination is beginning.

Interview of Xiaoqing Zheng

40. On August 1, 2018, agents with the FBI interviewed Zheng during the execution of the search warrant for his residence. During the interview Zheng made a number of oral statements, including, in sum and substance:

- a.) that it was common knowledge that "MatLab" electronic files are General Electric's (GE's) property and that it would be unlawful to take such files without permission;
- b.) that it is normally very difficult to unlawfully take any of GE's proprietary property;
- c.) that despite the difficulties inherent in attempting to unlawfully take GE's property, he used the steganography process on July 5, 2018 to take multiple electronic files belonging to GE that contained data about turbine technology;
- d.) that he had previously used steganography on somewhere around 5-10 prior occasions to take materials that belonged to GE;

- e.) that the companies in China that he owns or works for work on the same technologies that he works on as GE engineer; and
- f.) that his companies in China are not yet profitable, but have received grant money / funding from the government of China.

OFFENSE ALLEGED

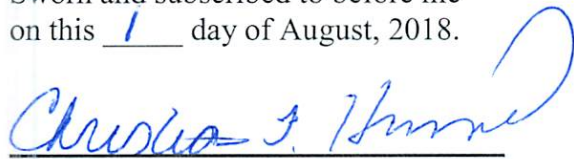
41. Based upon my experience, training, and the totality of circumstances in the above information, there is probable cause to believe that:

a.) On or about July 5, 2018, in the Northern District of New York, Xiaoqing Zheng, the defendant, with the intent to convert a trade secret that is related to a product and service used in and intended for use in interstate and foreign commerce, specifically "Steam Turbine Path Flow" technology, to the economic benefit of a person, or persons, other than the trade secret's owner, and knowing that the offense will injure any owner of that trade secret, knowingly did steal such information, all in violation of 18 U.S.C. § 1832(a)(1).



M.D. McDonald
Special Agent, FBI

Sworn and subscribed to before me
on this 1 day of August, 2018.



The Honorable Christian F. Hummel
United States Magistrate Judge
Northern District of New York